UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/932,982	08/21/2001	Todd Lagimonier	003636.0115	6823

7590	03/03/2006

MANELLI DENISON & SELTER PLLC
ATTN: William H Bollman
2000 M Street NW
Suite700
Washington, DC 20016

EXAMINER
SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	09/932,982	LAGIMONIER ET AL.
Office Action Summary	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>02 February 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-43</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-43</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claims 1-43 have been considered. The examiner maintains both prior art rejections.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR

1.17(e), was filed in this application after final rejection. Since this application is eligible for continued

examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the

finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's

submission filed on 8/29/05 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claims 36-43 are rejected under 35 U.S.C. 112, second paragraph. Claim 36 recites the

limitation "said largest sequence number yet seen". There is insufficient antecedent basis for this

limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for

the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or
in public use or on sale in this country, more than one year prior to the date of application for
patent in the United States.

Claims 1-43 are rejected under 35 U.S.C. 102(b) as being anticipated by anticipated by Hughes

(Hughes, J. "Combined DES-CBC, HMAC and Replay Prevention Security Transform". IPsec Working

Group. June 1996).

As per claims 1-43, the applicant describes a method of processing messages comprising the

following limitations which are met by Hughes:

a) determining a largest nonce value yet seen from a plurality of nonce values of out-of-order

messages (pages 3-4 and 10-11);

b) comparing a nonce value of a received message with said largest nonce value yet seen (pages

3-4 and 10-11);

c) comparing said nonce value to an acceptance window in response to said nonce value not

exceeding said largest nonce value yet seen (pages 3-4 and 10-11);

d) rejecting said received message in response to said nonce value falling outside said

acceptance window (pages 3-4 and 10-11).

Hughes discloses the idea of a sliding acceptance window to allow a receiver to accept out-of-

order nonce values while preventing replay attacks (pages 3-4). Appendix A (pages 10-11) illustrates the

procedure.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as
set forth in section 102 of this title, if the differences between the subject matter sought to be
patented and the prior art are such that the subject matter as a whole would have been obvious
at the time the invention was made to a person having ordinary skill in the art to which said
subject matter pertains. Patentability shall not be negatived by the manner in which the invention
was made.

Claims 1-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S.

Patent No. 5,970,143.

As per claims 1,10, and 19, the applicant describes a method of processing messages

comprising the following limitations which are met by Schneier:

a) determining a largest nonce value yet seen from a plurality of nonce values of out-of-order

messages (Col 16, lines 9-16);

b) comparing a nonce value of a received message with a largest nonce value yet seen (Col 16,

lines 9-16);

c) comparing said nonce value to an acceptance window in response to said nonce value not

exceeding said largest nonce value yet seen (Col 16, lines 17-32);

d) rejecting said received message in response to said nonce value falling outside said

acceptance window (Col 16, lines 17-32);

Schneier discloses all the limitations of the above claim. However, Schneier discloses limitations

a and b in one embodiment where sequence numbers are checked and limitations c and d in a second

embodiment where a timestamp is checked to make sure the message is within an acceptable time

window.

Combining the two embodiments would mean that a message is first checked against the stored

largest nonce value yet seen to make sure the newly-received sequence number is one larger. If the

newly-received sequence number is one larger it can be accepted as fresh. If the newly-received

sequence number does not exceed the largest nonce value yet seen, it is then checked against an

acceptance window by the timestamping operation and rejected if it fails this test.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

combine the two embodiments together because doing so allows old messages which are valid to be

allowed if they are within a certain time window. This makes the system more robust because it is now

able to allow out-of-order messages received within a certain time window.

As per claim 28, the applicant describes a system for processing messages in a peer-to-peer configuration comprising the following limitations:

a) a first peer configured to provide secure communication (14 of Fig 2);

b) a second peer configured to provide said secure communication (12 of Fig 2);

c) a secure communication module configured to be executed by said first peer and second peer, wherein said secure communication module is configured to:

i) determine a largest nonce value yet seen from a nonce value of a received message (Col 16, lines 9-16);

ii) compare said nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen (Col 16, lines 24-32);

iii) compare said nonce value to a replay mask (Col 16, lines 24-32);

iv) accept said received packet in response to said comparison of said nonce value and said replay mask being false (Col 16, lines 24-32);

The filter is the acceptance window and is comprised of a time limit of acceptance and unexpired messages within that time limit of acceptance which are replay masks to prevent the same nonce from being sent twice. If the nonce is not the largest nonce value yet seen and the time associated with the nonce is within a certain acceptable time limit, it is compared to unexpired messages within the time limit and accepted if the nonce value is not equal to a replay mask value already received.

As per claim 36, the applicant describes an interceptor device for processing messages comprising the following limitations:

a) a network interface (20 of Fig 2; Col 11, lines 56-58);

b) an expected sequence register configured to enumerate an expected sequence number of a packet received from a second network device (Col 16, lines 9-16);

c) a memory configured to store a replay mask (Col 16, lines 24-32);

d) a controller, wherein said controller is configured to:

i) determine a largest nonce value yet seen from a nonce value of a received message

(Col 16, lines 9-16);

ii) compare said nonce value to a filter in response to a sequence number of a received

packet via said network interface does not exceed a largest sequence number yet seen retrieved

from said expected sequence register (Col 16, lines 24-32);

iii) compare said sequence number to said replay mask retrieved from said memory (Col

16, lines 24-32);

iv) accept said received packet in response to said comparison of said sequence number

and said replay mask is false (Col 16, lines 24-32);

As per claims 2,3,11,13,20,21,29, and 37, the applicant discloses the method of claims

1,10,19,28, and 36, which are met by Schneier (see above), further comprising the following limitation

which is also met by Schneier:

Designating said nonce value as said largest nonce value yet seen in response to said nonce

value exceeding said largest nonce value yet seen (Col 16, lines 9-16);

As disclosed by Schneier, "The central computer stores the most recent sequence number in

memory" (Col 16, lines 13-14).

As per claims 4,12,22,30, and 38, the applicant discloses the method of claims 1,10,19,28, and

36, which are met by Schneier (see above), further comprising the following limitation which is also met

by Schneier:

Adjusting an acceptance window based on said nonce value exceeding said largest nonce value

yet seen (Col 16, lines 24-32);

The acceptance window is a log of nonces which have been received within a prescribed amount

of time. The acceptance window is used to determine a replay attack through two methods: 1) if the

nonce received has a time earlier than the acceptance window allows and 2) if the nonce received has

already been received and is stored in the acceptance window.

If the nonce received has a value exceeding the largest nonce value yet seen and is accepted as a valid nonce, it is stored in the database of nonces received. The acceptance window is adjusted because the acceptance window will no longer allow the nonce that has just been placed in it.

As per claims 5,7,14,16,23,25,32,34,40, and 42, the applicant describes the method of claim 1,6,10,16,19,24,28,33,36, and 41, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Designating said received message as a replay attack (Col 16, lines 17-32);

If the acceptance window determines that a message either 1) has a time earlier than the acceptance window allows or 2) has a nonce which has already been received and stored in the acceptance window, the message is determined to not be fresh. If a message is not fresh, it is a replay attack.

As per claims 6,8,15,17,24,26,33, and 41, the applicant describes the method of claims 1,10,19,28, and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

a) comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window (Col 16, lines 24-32);

b) rejecting said received message in response to an outcome of said comparison of said nonce value to said window mask value being true (Col 16, lines 24-32);

If the nonce value has a time which falls within the acceptance window, it is compared to window mask values to determine if the nonce has already been used. If the nonce value has already been used, the message is rejected. If the nonce has not already been used, the message is accepted.

As per claims 9,18, and 27, the applicant describes the method of claims 8,17, and 26, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Designating said nonce value as a nonce value seen (Col 16, lines 24-32);

As disclosed by Schneier, "The central computer maintains a database of all random numbers received from the game computers" (Col 16, lines 26-27).

As per claims 31 and 39, the applicant describes the system according to claims 28 and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Wherein said secure communication module is further configured to reject said received packet in response to said nonce value falling outside said filter (Col 16, lines 17-32);

The nonce value falls outside a filter and is rejected as a replay attack if the nonce's associated time is prior to the acceptable time of the filter.

As per claims 35 and 43, the applicant describes the system according to claims 28 and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Wherein said secure communication module is further configured to reject said received packet in response to said nonce value fails to fall within said filter and said secure communication module is further configured to designate said received packet as part of a replay attack (Col 16, lines 17-32).

Response to Arguments

Applicant's arguments, see Remarks, filed 2/2/06, with respect to the 112, second paragraph, rejection of claims 1-27 and 1-35 for lacking antecedent basis for "said received out-of-order message" and "said nonce value" have been fully considered and are persuasive. The 112, second paragraph, of claims 1-27 and 1-35 has been withdrawn.

Applicant's arguments with respect to the 112, second paragraph, rejection of claims 36-43 have been fully considered but they are not persuasive. Examiner still finds no antecedent basis for the limitation "said largest sequence number yet seen".

Applicant's arguments with respect to the 102(b) rejection of claims 1-43 under Hughes have

been fully considered but they are not persuasive. Applicant presents the following argument:

(1) The software routine beginning on page 10 is for in-order packets

Examiner respectfully disagrees with the above submits that Hughes clearly and explicitly

discloses that the software routine beginning on page 10 (i.e. Appendix A) is for out-of-order packets:

"An example may allow the most recent 32 packets to be allowed **to arrive out of order**. That is,
these 32 packets can arrive in any sequence relative to each other except that these packets are
guaranteed to arrive only once. **Appendix A** has actual code that implement a 32 packet replay window
and a test routine. The purpose of this routine is to show how it could be implemented" (page 3, bottom
four lines to page 4, top two lines).

Analysis of Appendix A further illustrates that it allows packets to arrive out-of-order. Examiner

has provided line numbering for Applicant's convenience. Hughes discloses that a nonce value (seq) of a

message, which may be out-of-order, is compared with a largest nonce value yet seen (lastseq) in line 2

of page 10. If the nonce value (seq) is larger than a largest nonce value yet seen, the method proceeds

with lines 2-9. Examiner notes, in particular, that the difference between the nonce value and the largest

nonce value yet seen is compared with ReplayWindowSize in line 4. In the instant case

ReplayWindowSize is 32. If the difference between the nonce value and the largest nonce value yet seen

is greater than 32 (for example, "seq" = 80 and "lastseq" = 1,000), the method acknowledges that the

packet is "way larger" than it should be in line 6. In line 7, the nonce value (seq) replaces lastseq.

Further, if the nonce value (seq) is not larger than the largest nonce value yet seen (lastseq), the

difference is compared to the ReplayWindowSize (i.e. 32 in this routine) to see if the nonce value is too

old (line 11) or if it has already been seen (line 12). **Finally, the routine ends by concluding that the**

packet is out of order but good (line 14). Thus, it is quite clear that Appendix A is not only for in-order

packets as suggested by Applicant.

Applicant's arguments with respect to the 103(a) rejection of claim 1 under Schneier have been

fully considered but they are not persuasive. Examiner has rejected claim 1 based on an obvious

combination of two procedures presented in Schneier. Since it is unclear whether Schneier expressly

intended the two procedures to take place together, Examiner has rejected claim 1 under single reference 103(a) and provided motivation for the combination. Applicant presents the following argument:

(1) no motivation for combination

Specifically, Applicant alleges that Examiner has correctly acknowledged that Schneier fails to even mention out-of-order messages (Remarks, page 4, lines 17-18). Further, Applicant argues that Examiner has picked and choosed elements to arrive at the claimed invention and that the combination would not have been obvious given the fact that Schneier should have combined the routines if they were obvious.

Examiner respectfully disagrees with such an argument. For the record, Examiner never indicated that Schneier fails to mention out-of-order messages as alleged by Applicant (Remarks, page 4, lines 17-18). The combination of the two routines of Schneier meet each and every limitation of the claimed invention. With regards to Applicant's motivation argument, the first procedure (Col 16, lines 9-16) discloses determining a largest nonce value yet seen by comparing a nonce value of a received message with a largest nonce value yet seen. However, in a second procedure, Schneier also contemplates that out-of-order nonce values may still be valid, despite their being out-of-order, if the nonce value is fresh (i.e. has not already been received and stored in a database) (Col 16, lines 26-32). Assuming that Schneier did not expressly intend the procedures to take place together, there is clear motivation to combine the procedures because doing so makes a method using the first procedure more robust by allowing for valid out-of-order messages to still be received as valid.

Thus, Examiner respectfully disagrees with Applicant's arguments that Examiner has arbitrarily picked and choosed elements of different embodiments to arrive at the claimed invention. Rather, Examiner has combined two procedures which have a clear motivation for combination. Further, assuming Schneier did not expressly intend the procedures to take place together, the mere statement that Schneier has not expressly combined two procedures does not preclude there being motivation for combination. In the instant case, motivation for combination exists, and Examiner has relied on such motivation accordingly.

Application/Control Number: 09/932,982   Page 11
Art Unit: 2137

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER